IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES FOR:

A WARRANT TO SEARCH THE RESIDENCE LOCATED AT 1025 CHURCH STREET, APARTMENT A, LYNCHBURG, VA 24504

Magistrate No. 6:21mj38
[UNDER SEAL]

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH AND SEIZURE WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, Brianna Maria Coleman, having been duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant to search the premises known as 1025 Church Street, Apartment A, Lynchburg, VA 24504, hereinafter the "**TARGET RESIDENCE**," further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent of Homeland Security Investigations (HSI) Immigration and Customs Enforcement (ICE), United States Department of Homeland Security. As such, I am an "investigative or law enforcement officer of the United States" within the meaning of Title 18, United States Code, Section 2510(7), that is, I am an officer of the United States, who is empowered by law to conduct investigations of, and make arrests for, controlled substance offenses enumerated in Title 21, United States Code.

3. I am currently assigned to the HSI Pittsburgh Office of the Assistant Special Agent in Charge in the Contraband Smuggling Group and have been so employed since June 2010. As a Special Agent, I am authorized to conduct investigations of alleged violations of immigration laws and customs laws, including offenses involving the importation of prohibited items, such as narcotics, under Titles 18, 19, and 21 of the United States Code. While being trained as a Special Agent of HSI, your affiant has received basic training at the Federal Law Enforcement Training Center located in Glynco, Georgia. Your affiant has participated in a number of narcotics and money laundering investigations which have resulted in the seizure of illegal drugs and evidence of drug violations, as well as the seizure of assets acquired with drug proceeds. Your affiant has conducted covert surveillance of suspected drug traffickers on numerous occasions, interviewed numerous individuals involved in the drug trafficking trade, participated in a Title III wiretap investigation, participated in the execution of numerous search and arrest warrants, assisted in the arrest of narcotics traffickers, and assisted in the seizure of controlled substances. Based upon the above experience, your affiant is familiar with the modus operandi of persons involved in illicit distribution of controlled substances, as well as the terminology used by persons involved in the illicit distribution of controlled substances. Your affiant is aware that persons involved in the illicit distribution of controlled substances routinely attempt to conceal their identities, as well as the location at which drug transactions take place.

4. Prior to joining HSI, I previously worked for the Pennsylvania Office of Attorney General, Bureau of Consumer Protection, from June 2006 to May 2010. As a Consumer Protection Agent, I investigated and enforced Pennsylvania consumer protection laws. In 2006, I

received a Bachelor of Arts degree in Government and History from Arcadia University in Glenside, Pennsylvania.

5. The facts and information contained in this affidavit are based upon my personal participation in this investigation and information provided by other law enforcement officers involved in this investigation. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, this affidavit does not set forth each and every fact learned by me during the course of this investigation.

6. In a substantial number of residential searches executed in connection with the drug investigations in which I and fellow HSI Agents and other investigators have been involved, the following kinds of drug-related evidence have typically been recovered from the residences of drug-traffickers:

a. Controlled substances, such as marijuana, heroin, crack cocaine, powder cocaine, methamphetamine, designer drugs (e.g., MDMA, a/k/a "ecstasy"), and synthetic narcotics, such as fentanyl;

b. Paraphernalia for packaging, processing, diluting, weighing, and distributing controlled substances, such as scales, funnels, sifters, grinders, glass panes and mirrors, razor blades, plastic bags, microwave ovens, heat-sealing devices, and dilutants such as mannitol, mannite, and vitamin B12;

c. Books, records, receipts, notes, ledgers, and other papers relating to the distribution of controlled substances;

d. Personal books and papers reflecting names, addresses, telephone numbers, and other contact or identification data relating to the distribution of controlled substances;

e. Cash, currency, and records relating to controlled substances income and expenditures of money and wealth, for example: money orders, wire transfers (Western Union), cashier's checks and receipts, bank statements, passbooks, checkbooks, and check registers, as well as precious metals such as gold and silver, and precious gems such as diamonds;

f. Documents indicating travel in interstate and foreign commerce such as travel itineraries, plane tickets, boarding passes, motel and hotel receipts, passports and visas, credit card receipts, telephone bills and rental car agreements;

g. Mobile electronic communication devices, such as cellular telephones and "smart phones", electronic messaging equipment, such as tablets, pagers, telephones answering machines, and their tapes, electronic storage devices, such as GPS devices and portable media players, and other such mobile electronic devices that store data, as well as the content therein;

h. Firearms and other dangerous weapons; and

i. Photographs, in particular, photographs of co-conspirators, assets, and/or drugs.

7. In addition, during the course of such residential searches, I and other agents have also found items of personal property that tend to identify the person(s) in the residence, occupancy, control, or ownership of the subject premises. Such identification evidence is typical

of the articles people commonly maintain in their residences, such as canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, utility and telephone bills, statements, identification documents, and keys to safe deposit boxes and storage facilities.

8. Based upon my training and experience, as well as the knowledge and experience of other agents and police officers involved in this investigation, I am aware that it is generally a common practice for drug traffickers to store their drug inventory and drug-related paraphernalia (as described above) in their residences. Further, it is generally a common practice for drug traffickers to maintain in their residence(s) their business records relating to their drug trafficking activities. Because drug traffickers in many instances will "front" (that is, sell on consignment) controlled substances to their clients, or alternatively, will be "fronted" controlled substances from their suppliers, such record-keeping is necessary to keep track of amounts paid and owed, and such records will also be maintained close at hand so as to readily ascertain current balances. Often drug traffickers keep "pay and owe" records to show balances due for drugs sold in the past ("pay") and for payments expected ("owe") as to the trafficker's supplier and the trafficker's dealer(s). Additionally, drug traffickers must maintain telephone and address listings of clients and suppliers and keep them immediately available in order to efficiently conduct their drug trafficking business.

9. Based upon my training and experience, I also am aware that it is generally a common practice for traffickers to conceal at their residences and/or their business large sums of money, either the proceeds from drug sales or money to be used to purchase controlled substances. Drug traffickers must maintain on hand the large amounts of United States currency in order to maintain and finance their ongoing narcotics business. In this connection, drug

traffickers typically make use of wire transfers, cashier's checks, and money orders to pay for controlled substances. Evidence of such financial transactions and records relating to income and expenditures of money and wealth in connection with drug trafficking would also typically be maintained in residences and/or their business.

10. Based upon my training and experience, I know that drug traffickers commonly have in their possession, that is on their person, at their residences and/or their business, firearms, including but not limited to handguns, pistols, revolvers, rifles, shotguns, machine guns and other weapons. I also am aware that, typically, drug traffickers possess these firearms and other dangerous weapons to protect their profits, supply of drugs, and themselves from others who might attempt to forcibly take the traffickers' profits and/or supply of drugs.

11. Further, I am aware that narcotics traffickers maintain books, records, receipts, notes, ledgers, airline tickets, money orders, and other papers relating to the transportation, ordering, sale and distribution of controlled substances. Furthermore, I know that the aforementioned books, records, receipts, notes, ledgers, etc. are generally maintained where the traffickers have easy and ready access to them, including in their residences, businesses, and automobiles.

12. Further, I am aware that persons involved in significant drug trafficking conceal in their residences, businesses, and automobiles, large amounts of currency, financial instruments, precious metals, jewelry, and other items of value and/or proceeds of drug transactions and evidence of financial transactions relating to obtaining, transferring, secreting, or spending large sums of money derived from narcotic trafficking activities.

13. When drug traffickers amass proceeds from the sale of drugs, drug traffickers often attempt to legitimize these profits, or otherwise conceal them from discovery by law enforcement officers. To accomplish these goals, drug traffickers often use different techniques, including but not limited to foreign and domestic banks and their attendant services, securities, cashier's checks, money drafts, letters of credit, brokerage houses, the purchase of real estate, as well as shell corporations and business fronts to conceal the true ownership and illegal source of the proceeds.

14. Further, I am aware that drug traffickers commonly maintain books or papers that reflect names, addresses and/or telephone numbers of their associates in the trafficking organization. Drug traffickers also take or cause to be taken photographs of themselves, their associates, their property, and their product and usually maintain these photographs in their possession.

15. Further, I am aware that drug traffickers usually keep paraphernalia for packaging, cutting, weighing, and distributing narcotics. Such paraphernalia includes, but is not limited to scales, plastic bags, cutting agents, and other devices used for packaging to aid in the concealment of the drug for its distribution.

16. Further, I am aware that drug traffickers often operate under assumed names in order to conceal their true identities from law enforcement officers. In so doing, they acquire property, services, and personal identification (such as driver's licenses and birth certificates) under their assumed or alias names; and that they maintain such documents as evidence of their false identities in their residences, businesses, and automobiles together with evidence of their true identities.

17. I have knowledge that drug traffickers commonly conceal their activities from members of the public by transacting their business in a covert manner and frequently conduct their business during the nighttime hours when darkness helps conceal their activities. Moreover, it is highly unusual for individuals primarily engaged in drug trafficking activities to associate in their businesses or social activities with others not engaged in the same drug trafficking activities.

18. I know that it is common for drug dealers to secret contraband, proceeds of drug sales, and records of drug transactions in secure locations within their residence and/or their business, for their ready access and to conceal them from law enforcement authorities.

19. My awareness of these drug trafficking practices, as well as my knowledge of drug use and distribution techniques as set forth in this affidavit, arise from the following:

a. My own involvement in prior drug investigations and searches during my career as a law enforcement officer, as previously described;

b. My involvement on a number of occasions in debriefing confidential informants and cooperating individuals in prior drug investigations, as well as what other agents and police officers have advised me when relating the substance of their similar debriefings and the results of their own drug investigations;

c. Discussion with other members of HSI and law enforcement officers, both about the facts of this case in particular and about trafficking in general; and

d. Other intelligence information provided through law enforcement channels.

FACTS ESTABLISHING PROBABLE CAUSE

20. HSI, along with assistance from the United States Postal Inspection Service (USPIS) and the Pennsylvania State Police (PSP) are conducting an investigation into the distribution of narcotics into Western Pennsylvania by a subject identified as Matthew TERRELL.

21. On April 18, 2020, U.S. Customs and Border Patrol (CBP) at JFK International Airport seized a parcel entering the United States from the Netherlands that was addressed to "Riggs Visser, 715 Clear Ridge Road, Artemas, PA 17211". The parcel was found to contain 112 grams of suspected MDMA (also known as, "Ecstasy"). Subsequent lab testing confirmed that the substance was, in fact, MDMA, and that it weighed 100.54g.

22. On June 18, 2020, CBP agents at JFK seized another parcel addressed to "Riggs Viser" at "715 Clear Ridge Road, Artemas, PA 17211."

23. During this occasion, CBP agents at JFK Airport were conducting an "enforcement examination of mail shipped from Netherlands, [and] K9 Bence #160608 alerted to this package. The bulky envelope was examined and found to contain a tan rock-like substance secreted within a plastic pouch." CBP agents conducted a field test on the substance which returned a positive indication for MDMA. The suspected MDMA weighed approximately 61 grams. The parcel bore multiple stamps instead of a USPS tracking number.

24. The June parcel looked very similar in appearance to the parcel seized in April.

25. Because the June parcel was destined for an address in the Western District of Pennsylvania, CBP agents contacted HSI agents and provided the parcel to them to conduct a controlled delivery.

26. Your Affiant applied for and received search warrants to conduct the controlled delivery, which were signed by United States Magistrate Judge Keith A. Pesto at Magistrate Numbers 3:20-123MJ, 3:20-124MJ, and 3:20-125MJ.

27. On June 23, 2020, investigators executed a successful controlled delivery of the parcel[1] and subsequent search warrant at the residence in Artemas, PA. Inside the residence, agents encountered Riggs VISSER's mother. Riggs VISSER was not present. VISSER's mother showed agents to Riggs's room in the basement. Inside the room agents located quantities of several hallucinogenic drugs, including, approximately 49 grams of psilocin mushrooms, a capsule containing 302mg of dimethyltryptamine (DMT), and approximately 40 "hits" of lysergic acid diethylamide (LSD).

28. While executing the warrant, investigators encountered and interviewed a Confidential Source ("CS1")[2]. CS1 indicated that VISSER's source of supply was a male named Matt TERRELL. CS1 advised that VISSER had purchased the MDMA that had been the subject of the controlled delivery from TERRELL. CS1 provided a phone number for TERRELL (which subscriber information and a subsequent border search (discussed below) confirmed belonged to TERRELL), identified a photo of TERRELL, provided the address of TERRELL's

---

1 Following the controlled delivery, the suspected MDMA from the interdicted parcel was sent for laboratory testing. Lab testing confirmed that it did, in fact, contain approximately 50 grams of MDMA.

2 CS1's identity is known to your affiant. CS1 is a known drug user. CS1 is cooperating for consideration on anticipated criminal charges. Nonetheless, your affiant believes the information provided by CS1 is credible and reliable based on my ability to corroborate, through the use of subpoenas and other legal process, surveillance, and interviews with other law enforcement agents/officers, much of the information CS1 provided.

apartment in Oregon where he had been living, told investigators where TERRELL went to college, provided bank transfer information used by TERRELL, and more.

29. Based on information provided by CS1, multiple Grand Jury subpoenas were issued to obtain records, including several subpoenas directed to Early Warning Services (EWS), the company that operates Zelle, a mobile payment application that allows peer-to-peer (P2P) money transfers. According to CS1, TERRELL occasionally used Zelle to receive payment from his drug purchasers, including from VISSER.

30. Your Affiant is aware that a Zelle user must provide an email address or phone number to sign up for a Zelle account. EWS provided responsive documents that showed TERRELL had both an email address and a phone number on file. The phone number associated with TERRELL's Zelle account, 252-256-2862, was the same phone number provided for TERRELL by CS1. Further, the email address associated with the account is mattterrell11@gmail.com.

31. Early Warning Services/Zelle records showed the following relevant transactions:

- On April 6, 2020, Riggs VISSER sent a payment of $2,350.00 to TERRELL at BB&T Bank.
- On May 8, 2020, Riggs VISSER sent a payment of $1,000.00 was sent to TERRELL at BB&T Bank.

32. As stated previously, agents seized 100 grams of MDMA from a parcel addressed to "Riggs Visser," on April 18, 2020 and conducted the controlled delivery of 50 grams of MDMA to VISSER's residence on June 23, 2020. Based on the time frame of the seizures and information from CS1, I believe the Zelle transfers listed above were payment for drugs, specifically, MDMA. I believe the Zelle transfer on April 6, 2020 was for the 100-gram (4-

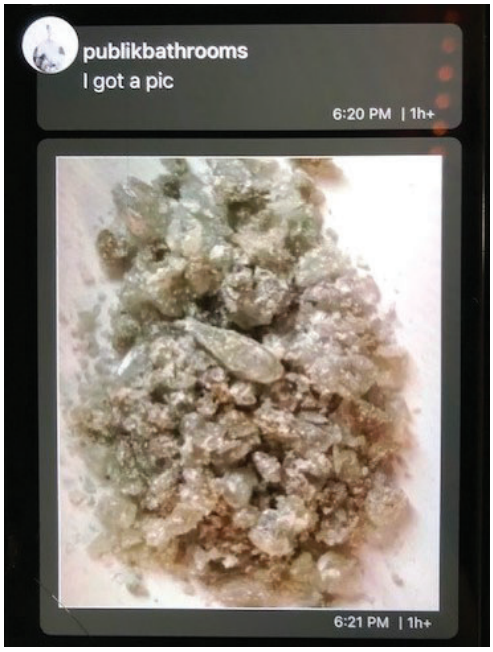
ounce) quantity that was seized. I believe the second transfer on May 8, 2020 was for a 50-gram replacement parcel, due to the first parcel's seizure. Indeed, CS1 advised that this was the case.

33. As part of the investigation, a Grand Jury subpoena was also issued to BB&T Bank. BB&T Bank provided information, including statements for a bank account in TERRELL's name along with who investigators believe is TERRELL's father, at what investigators believe to be TERRELL's parent's address. These statements show the deposits of the Zelle transfers listed above into an account ending 7516. The bank records show multiple Zelle transfers into and out of this bank account. Further, TERRELL apparently used this account for other payments of expenses, including to the apartment complex in Oregon where he lived for a period.

34. In October 2020, investigators attempted to make a controlled purchase of MDMA, known as "M" or "molly" in the drug community from TERRELL using CS1. At the direction of law enforcement officers, CS1 communicated with TERRELL over an encrypted application (Wickr) to arrange the transaction. On the Wickr app, TERRELL used the moniker "publikbathrooms." During one of these conversations on October 12, 2020, screenshots of which agents possess and your affiant has reviewed, CS1 inquired about the price of the MDMA. TERRELL replied, "It's 1k a oz to me rn lol". In the next message, TERRELL wrote "And it's cola molly". Based on my training, experience, and knowledge of the investigation, Your Affiant understands this to mean that TERRELL was paying $1,000 per ounce of MDMA to which he would then attach an upcharge in order to sell it for a profit. Further, your affiant knows "cola molly" to refer to a specific type of MDMA which is brown in color.

35. TERRELL and CS1 later discussed payment and TERRELL advised CS1 that "its ok to send it via Zelle" and that "Cash app [sic] is cool too".

36. TERRELL also sent CS1 a photo of the presumed MDMA:



37. Your Affiant is aware from discussions with CS1 that TERRELL often utilized encrypted messaging platforms, such as Wickr, to communicate with him/her and, presumably, other customers. Your Affiant is aware that those involved in illicit activities oftentimes utilize these platforms so the contents of their chats cannot be intercepted by law enforcement. Many such apps only retain the message for a short period of times and others self-destruct.

38. In a later conversation about the controlled purchase of drugs, TERRELL requested that CS1 provide payment via Bitcoin. Your Affiant is aware that cryptocurrencies, which are digital currencies, are favored among many involved in illicit activities because it involves the online transfer of these digital funds and the users remain largely anonymous. As part of the investigation, grand jury subpoenas have been issued to multiple cryptocurrency

exchange platforms, e.g. Binance, Coinbase, and RobinHood. Records received from Coinbase and Binance, as well as other financial records from PayPal, show that over time, including during the period in which TERRELL was involved with CS1, TERRELL engaged in numerous cryptocurrency transactions.

39. On November 3, 2020, agents/officers issued $1,500 of official funds to CS1, to be transferred via Zelle to TERRELL at phone number 252-256-2862 for the controlled purchase of MDMA. Agents also provided CS1 a P.O. Box address to which CS1 was to direct TERRELL to send the MDMA.

40. On November 3, 2020, CS1 transferred the official funds to TERRELL via Zelle. In a message received that same day, TERRELL told CS1, "Word i got your Zelle", indicating that the Zelle transfer of controlled funds had been successful. TERRELL also wrote, "Yuh once i turn this money into fucking btc (Bitcoin) I want some of this m lol", which your Affiant understands to mean that TERRELL wanted to try some of the MDMA he was having shipped to CS1. On November 6, 2020, TERRELL provided CS1 with a photo of a USPS receipt with tracking information. The receipt was from a Marina Del Ray, CA Post Office.

41. The tracking information provided by TERRELL showed that the parcel was to arrive at the designated P.O. Box at the South Side, Pittsburgh Post Office on Friday, November 6, 2020. However, a search for the parcel the following week, along with updated tracking, showed the parcel had been returned to California due to a delivery address error. Investigators attempted to locate and seize the parcel but were unsuccessful.

42. At agent's/officer's direction, CS1 contacted TERRELL regarding the lost package. During the conversation, TERRELL sent photos of the conversation between he

(TERRELL) and his source of supply (SOS) on what appears to be a different phone. In an undated message which TERRELL sent a photo of to CS1, on or about November 23, 2020, the SOS wrote, "Bro your dumb ass client sent that shit to a bando [abandoned house] or something." Later, regarding the return address on the lost parcel, which investigators were unable to identify, "i mean its at this fuckin work center near my homies house i guess HE gets mail there". The messages between TERRELL and the SOS continued with the parties discussing their hesitance to undertake efforts to locate the package out of concerns that it could result in their arrest.

43. At law enforcement direction, CS1 inquired whether TERRELL would arrange for a replacement to be shipped due to the original parcel's return to sender. TERRELL sent screen shots of his (TERRELL's) conversations with his SOS. In these messages, the SOS blamed CS1 for providing an invalid address and declined to ship a replacement parcel.

44. As part of the investigation, additional Grand Jury subpoenas were issued to Early Warning Services for records related to the Zelle transfer involved in the unsuccessful controlled purchase, as well as more recent bank account information.

45. The EWS/Zelle subpoena response showed that TERRELL did, in fact, receive the $1,500.00 in official funds on November 3, 2020. The response showed that the funds again went to TERRELL's bank account at BB&T Bank.

46. In early June 2021, your Affiant learned that TERRELL took an international trip to Mexico. On June 8, 2021, your Affiant was notified by HSI SA Michael MacBride from HSI Romulus, MI that TERRELL had made entry into the United States via air from Cancun, Mexico. Agents conducted a border search of TERRELL at his point of entry in Michigan.

During the search, TERRELL was found in possession of a cell phone and two laptops. TERRELL declined to provide the passcode for his cell phone to investigators. Due to this and the ongoing investigation, the electronics were mailed to HSI Pittsburgh in order to continue the border search for electronic contraband evidence.

47. On June 15, 2021, your Affiant received the electronics and provided them to HSI Computer Forensics Agent (CFA) Dave Coleman for the border search. CFA Coleman began the search on the same day.

48. Because the passcode was not provided for the cell phone, only a partial extraction could be obtained. An extraction of the Microsoft laptop and the MacBook were not possible due to password protection. Following the partial extraction from the cell phone, the devices were returned to TERRELL.

49. On July 16, 2021, your Affiant began reviewing the partial download of TERRELL's iPhone. Your affiant found the following email addresses, monikers, and phone number associated with the phone: matthew.terrell@student.gcccks.edu; mattterrell11@gmail.com; and 252-256-2862, in addition to others. The moniker publikbathrooms and the phone number were previously known to be used by TERRELL. The phone number and an email address were the same as associated with TERRELL's Zelle account and the phone number was the same as provided by CS1.

50. From the partial extraction, your affiant also reviewed photos of drugs and conversations about drugs, to include drug lingo: "snow" (cocaine), "Shrooms" (mushrooms), "dabs" (LSD), "m30s" (Oxycodone), and others, in addition to marijuana. Photos depicting large amounts of drugs and money were also observed. The phone data also included notes

explaining how to package and mail drugs and money, so as not to be susceptible to law enforcement detection. There were also many addresses, which is indicative of mailing drugs and money through the mail, as well as tracking numbers. Your affiant also viewed photos of guns, including handguns, rifles, and a couple AR rifles.

51. Present on the phone were several apps, encrypted sites, and content with known DarkNet sites and cryptocurrency, to include: Local Bitcoin, Tor, Torrent, Onion, ProtonMail, Privnote (messages will self-destruct), Binance, Coinmarketcap, and Robinhood. As stated above, your Affiant believes that those involved in illicit activities will oftentimes utilize encrypted messaging apps and cryptocurrency in order to insulate themselves from law enforcement detection.

52. Also found on the phone was a conversation between TERRELL and a contact labeled, "Stephen (juwan) Moye" with conversations up to the date of the phone's detention at the border. The parties appeared to engage in a detailed discussion about breaking into a drug stash house through various means (picking the lock, forcing their way in, etc.), stealing the safe, and tying up anyone who may be present, and beating them, if necessary. Further, they discussed bringing guns to commit the robbery and TERRELL said that he would bring his AR. In a message dated June 8, 2021, Publikbathrooms (TERRELL) wrote "I got my shit and a ar pistol" followed by, "But we can be killing anyone with those or leaving them anywhere (emojis) or I'll get locked". Since TERRELL's electronics were detained, it is unknown if he followed through with the discussed armed robbery.

53. Based on a review of the partially downloaded cell phone, your Affiant believes that TERRELL is heavily involved in drug trafficking with multiple persons. Further, as

indicated above, TERRELL has the means to commit and may also have a propensity toward violence.

54. Based on information from USPIS Postal Inspector Staci Johnson, your Affiant believes that TERRELL still utilizes his parents address in Harrisonburg, VA to receive paper mail. However, it is believed that TERRELL does not reside there.

55. Your Affiant is aware that those involved in illicit activities oftentimes try to insulate themselves from law enforcement detection by keeping multiple addresses separate from their permanent residence.

56. Your Affiant is aware that a recent report from the commercially available database, Accurint, showed that TERRELL is associated with the **TARGET RESIDENCE**.

57. On September 9, 2021, your Affiant again reviewed TERRELL's phone download. Your Affiant found that from September 24, 2020, through April 19, 2021, TERRELL made reference to the **TARGET RESIDENCE** approximately 11 times. TERRELL texted several contacts that the **TARGET RESIDENCE** was his address.

58. 1025 Church Street, Apartment A, Lynchburg, VA 24504, the **TARGET RESIDENCE**, is located within a large, three-story, yellow brick commercial/residential building. There are three doors at the center of the building. The door to the left is marked "1025A" over the door, the center door is marked "1025" over the door, and the door to the right is marked "1025B" over the door. Upon further viewing, the doors to the right and left appear to not be in use and have key locks at the top of both doors. During surveillance, all people accessing the building used the center door. Further, because the doors are glass, two additional doors were visible inside the center locked front door and those doors appear to allow access to

1025A and 1025B.

59. On November 2, 2021, HSI Task Force Officers (TFOs) Joe Timms and Robert Warman were conducting surveillance at the **TARGET RESIDENCE** and observed a black BMW pull up on the street. A white male, resembling TERRELL got out and traveled in the direction of the **TARGET RESIDENCE**. Investigators queried the registration of the vehicle and found that it was registered to TERRELL, at what investigators believe to be a former address.

60. On November 3, 2021, your Affiant, HSI SA Cody Schmitt, and TFOs Timms and Warman were again conducting surveillance at the **TARGET RESIDENCE**. TERRELL was seen coming from the direction of the **TARGET RESIDENCE** and got into the same BMW and departed from the area. Later that day, TERRELL was observed driving back to the **TARGET RESIDENCE** and then he walked into the center door of the residence (through which he would then be able to access 1025A). A short time later, TERRELL departed from the **TARGET RESIDENCE** with two other individuals and walked down the street. TERRELL was identified based on several photos of TERRELL that investigators had reviewed.

61. On November 4, 2021, the management company for the **TARGET RESIDENCE** confirmed to Your Affiant that TERRELL is a resident of 1025A and his door is the left-hand door accessed through the center door.

62. On November 4, 2021, your Affiant and another investigator served a DHS administrative subpoena on the management company of the **TARGET RESIDENCE**. On November 5, 2021, your Affiant received a portion of the lease from the management company,

which confirms that Matthew TERRELL is the current resident of the **TARGET RESIDENCE**. The current lease was signed on October 1, 2021, for a period of six months.

63. Based on the above described investigation, Your Affiant believes that evidence of violations of Title 21, United States Code, Section 841 (distribution and possession with intent to distribute controlled substances), 21 United States Code 846 (conspiracy), and Title 18, United States Code, Section 1956(h) (money laundering), (the TARGET OFFENSES), that being the possession with intent to distribute controlled substances as well as proceeds of the distribution of these controlled substances, will be located within the **TARGET RESIDENCE**.

64. Based on the above, your Affiant believes that the items, documents and records listed in Attachment B to the requested search warrant will constitute evidence, fruits and instrumentalities relating to the TARGET OFFENSES, that may be found at the **TARGET RESIDENCE**.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

65. As described above and in Attachment B, this application seeks permission to search for records that might be found in the **TARGET RESIDENCE**, in whatever form they are found. One form in which the records might be found at the **TARGET RESIDENCE** is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

a. *Probable cause.* I submit that if a computer or storage medium is found at the **TARGET RESIDENCE**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons: Based on

my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

66. *Forensic evidence.* As further described in Attachment B-1, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **TARGET RESIDENCE** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United

States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image

files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to purchase narcotics on the DarkNet or through other online vendors, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

66. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded

on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

67. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

68. Because several people may share the **TARGET RESIDENCE** as a residence, it is possible that the **TARGET RESIDENCE** will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this application could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

REQUEST FOR SEALING

69. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature

disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

CONCLUSION

70. I submit that this affidavit supports probable cause for a warrant to search the **TARGET RESIDENCE**, described in Attachment A and seize the items described in Attachment B.

The above information is true and correct to the best of my knowledge, information and belief.

/s/ Brianna M. Coleman
Brianna M. Coleman
Special Agent
Homeland Security Investigations

Sworn and subscribed before me, by telephone
pursuant to Fed. R. Crim. P. 4.1(b)(2)(A),
on November 8, 2021.

Robert S. Ballou

United States Magistrate Judge